CLAIMS

What is Claimed is:

1. A method of protecting communication security when using a key lease to re-authenticate after a primary authentication protocol has been performed, comprising the steps of:

a) performing a secondary authentication protocol between a client electronic system (client) and a network access point electronic system (AP) using said key lease; and

b) if said secondary authentication protocol is successful, generating a session encryption key for encrypting communication traffic between said client and said AP.

2. A method as recited in Claim 1 wherein said step a) includes the steps of:

transmitting said key lease from said client to said AP;

generating a first random number associated with said client and a second random number associated with said AP, wherein said key lease includes an encryption key for use in said secondary authentication protocol; and

transmitting said first random number to said AP and said second random number to said client.

3. A method as recited in Claim 2 wherein said step b) includes:

using said encryption key, said first random number, said second random number, and a hash function to determine said session encryption key.

4. A method as recited in Claim 3 wherein said step b) includes:

applying a HMAC-MD5 algorithm and said encryption key on a concatenation of said first random number and said second random number to determine said session encryption key.

5. A method as recited in Claim 3 wherein said step b) includes:

applying a HMAC-SHA-1 algorithm and said encryption key on a concatenation of said first random number and said second random number to determine said session encryption key.

6. A method as recited in Claim 2 wherein said step b) includes:

generating a first session encryption key for encrypting communication traffic from said client to said AP; and

generating a second session encryption key for encrypting communication traffic from said AP to said client.

7. A method as recited in Claim 6 wherein said step b) includes:

using said encryption key, said first random number, said second random number, a first media access control (MAC) address associated with said client, a

second media access control (MAC) address associated with said AP, and a hash function to determine said first and second session encryption keys.

8. A method as recited in Claim 7 wherein said step b) includes:

applying a HMAC-MD5 algorithm and said encryption key on a concatenation of said first random number, said second random number, said first media access control (MAC) address associated with said client, and said second media access control (MAC) address associated with said AP to determine said first session encryption key.

9. A method as recited in Claim 7 wherein said step b) includes:

applying a HMAC-SHA-1 algorithm and said encryption key on a concatenation of said first random number, said second random number, said first media access control (MAC) address associated with said client, and said second media access control (MAC) address associated with said AP to determine said first session encryption key.

10. A method as recited in Claim 7 wherein said step b) includes:

applying a HMAC-MD5 algorithm and said encryption key on a concatenation of said first random number, said second random number, said second media access control (MAC) address associated with said AP, and said first media access control (MAC) address associated with said client to determine said second session encryption key.

11. A method as recited in Claim 7 wherein said step b) includes:

applying a HMAC-SHA-1 algorithm and said encryption key on a concatenation of said first random number, said second random number, said second media access control (MAC) address associated with said AP, and said first media access control (MAC) address associated with said client to determine said second session encryption key.

12. An apparatus for re-authenticating using a key lease after a primary authentication protocol has been performed, comprising:

a client electronic system (client) configured to perform a secondary authentication protocol with a network access point electronic system (AP) using said key lease, wherein if said secondary authentication protocol is successful said client is configured to generate a session encryption key for encrypting communication traffic between said client and said AP.

13. An apparatus as recited in Claim 12 wherein said client is configured to transmit said key lease to said AP, wherein said client is configured to generate a first random number, wherein said key lease includes an encryption key for use in said secondary authentication protocol, wherein said client is configured to transmit said first random number to said AP and to receive a second random number from said AP.

14. An apparatus as recited in Claim 13 wherein said client is configured to use said encryption key, said first random number, said second random number, and a hash function to determine said session encryption key.

15. An apparatus as recited in Claim 14 wherein said client is configured to apply a HMAC-MD5 algorithm and said encryption key on a concatenation of said first random number and said second random number to determine said session encryption key.

16. An apparatus as recited in Claim 14 wherein said client is configured to apply a HMAC-SHA-1 algorithm and said encryption key on a concatenation of said first random number and said second random number to determine said session encryption key.

17. An apparatus as recited in Claim 13 wherein said client is configured to generate a first session encryption key for encrypting communication traffic from said client to said AP, and wherein said client is configured to generate a second session encryption key for encrypting communication traffic from said AP to said client.

18. An apparatus as recited in Claim 17 wherein said client is configured to use said encryption key, said first random number, said second random number, a first media access control (MAC) address associated with said client, a second media

access control (MAC) address associated with said AP, and a hash function to determine said first and second session encryption keys.

19. An apparatus as recited in Claim 17 wherein said client is configured to apply a HMAC-MD5 algorithm and said encryption key on a concatenation of said first random number, said second random number, said first media access control (MAC) address associated with said client, and said second media access control (MAC) address associated with said AP to determine said first session encryption key.

20. An apparatus as recited in Claim 17 wherein said client is configured to apply a HMAC-SHA-1 algorithm and said encryption key on a concatenation of said first random number, said second random number, said first media access control (MAC) address associated with said client, and said second media access control (MAC) address associated with said AP to determine said first session encryption key.

21. An apparatus as recited in Claim 17 wherein said client is configured to apply a HMAC-MD5 algorithm and said encryption key on a concatenation of said first random number, said second random number, said second media access control (MAC) address associated with said AP, and said first media access control (MAC) address associated with said client to determine said second session encryption key.

22. An apparatus as recited in Claim 17 wherein said client is configured to apply a HMAC-SHA-1 algorithm and said encryption key on a concatenation of said

first random number, said second random number, said second media access control (MAC) address associated with said AP, and said first media access control (MAC) address associated with said client to determine said second session encryption key.

23. An apparatus for re-authenticating using a key lease after a primary authentication protocol has been performed, comprising:

a network access point electronic system (AP) configured to perform a secondary authentication protocol with a client electronic system (client) using said key lease, wherein if said secondary authentication protocol is successful said AP is configured to generate a session encryption key for encrypting communication traffic between said client and said AP.

24. An apparatus as recited in Claim 23 wherein said AP is configured to receive said key lease and a first random number from said client, wherein said key lease includes an encryption key for use in said secondary authentication protocol, wherein said AP is configured to generate a second random number and to transmit said second random number to said client.

25. An apparatus as recited in Claim 24 wherein said AP is configured to use said encryption key, said first random number, said second random number, and a hash function to determine said session encryption key.

26. An apparatus as recited in Claim 25 wherein said AP is configured to apply a HMAC-MD5 algorithm and said encryption key on a concatenation of said first random number and said second random number to determine said session encryption key.

27. An apparatus as recited in Claim 25 wherein said AP is configured to apply a HMAC-SHA-1 algorithm and said encryption key on a concatenation of said first random number and said second random number to determine said session encryption key.

28. An apparatus as recited in Claim 24 wherein said AP is configured to generate a first session encryption key for encrypting communication traffic from said client to said AP, and wherein said AP is configured to generate a second session encryption key for encrypting communication traffic from said AP to said client.

29. An apparatus as recited in Claim 28 wherein said AP is configured to use said encryption key, said first random number, said second random number, a first media access control (MAC) address associated with said client, a second media access control (MAC) address associated with said AP, and a hash function to determine said first and second session encryption keys.

30. An apparatus as recited in Claim 29 wherein said AP is configured to apply a HMAC-MD5 algorithm and said encryption key on a concatenation of said first

random number, said second random number, said first media access control (MAC) address associated with said client, and said second media access control (MAC) address associated with said AP to determine said first session encryption key.

31. An apparatus as recited in Claim 29 wherein said AP is configured to apply a HMAC-SHA-1 algorithm and said encryption key on a concatenation of said first random number, said second random number, said first media access control (MAC) address associated with said client, and said second media access control (MAC) address associated with said AP to determine said first session encryption key.

32. An apparatus as recited in Claim 29 wherein said AP is configured to apply a HMAC-MD5 algorithm and said encryption key on a concatenation of said first random number, said second random number, said second media access control (MAC) address associated with said AP, and said first media access control (MAC) address associated with said client to determine said second session encryption key.

33. An apparatus as recited in Claim 29 wherein said AP is configured to apply a HMAC-SHA-1 algorithm and said encryption key on a concatenation of said first random number, said second random number, said second media access control (MAC) address associated with said AP, and said first media access control (MAC) address associated with said client to determine said second session encryption key.

34. A method of authenticating a client electronic system (client) to allow access to a network, comprising the steps of:

a) in response to a first request to authenticate, performing a primary authentication protocol between said client and a first network access point electronic system (first AP);

b) if said primary authentication protocol is successful, generating a key lease, wherein said key lease includes context information;

c) transmitting said key lease to said client; and

d) in response to a second request to authenticate, performing a secondary authentication protocol between said client and a second network access point electronic system (second AP) using said key lease.

35. A method as recited in Claim 34 further comprising the step of:

e) if said secondary authentication is successful, using said context information of said lease key to control access of said client to said network.

36. A method as recited in Claim 34 wherein said context information includes information established in said primary authentication protocol.

37. A method as recited in Claim 34 wherein said context information includes accounting information, session timeout information, and filtering information.

38. A method as recited in Claim 34 wherein said key lease further includes a first identifier associated with said client, a first encryption key associated with said primary authentication protocol, a second encryption key for use in said secondary authentication protocol, a key lease period for indicating a length of time in which said key lease is valid, integrity function data for determining an unauthorized change to a first portion of said key lease, and a second identifier associated with a particular network access point electronic system group of a plurality of network access point electronic system groups.

39. A method as recited in Claim 38 wherein said first portion includes said first identifier, said first encryption key, said second encryption key, said key lease period, and said context information.

40. A method as recited in Claim 38 wherein a second portion of said key lease is encrypted using a third encryption key.

41. A method as recited in Claim 40 wherein said second portion includes said first identifier, said first encryption key, said second encryption key, said key lease period, said context information, and said integrity function data.

42. A method as recited in Claim 40 wherein said step b) includes:

b1) transmitting said first identifier and said key lease to said second AP;

b2) if said second AP is associated with said second identifier of said key lease, retrieving said third encryption key corresponding to said second identifier; and

b3) decrypting said second portion of said key lease using said retrieved third encryption key.

43. A method as recited in Claim 42 wherein said step b) further includes:

b4) determining whether said first identifier transmitted by said client matches said first identifier decrypted from said key lease;

b5) determining whether said integrity function data decrypted from said key lease matches an integrity function performed on said first portion of said key lease;

b6) determining whether said key lease period has not expired; and

b7) if valid determinations are made in said steps b4) to b6), initiating said secondary authentication protocol between said client and said second AP.

44. A method as recited in Claim 34 wherein said secondary authentication protocol comprises a mutual challenge-response protocol based on symmetric encryption.

45. A method as recited in Claim 34 wherein said secondary authentication protocol comprises a mutual challenge-response protocol based on a one-way hash function message authentication code (HMAC) implementation.

46. A method as recited in Claim 34 wherein said secondary authentication protocol comprises a mutual challenge-response protocol based on a keyed message authentication code implementation.

47. An apparatus for performing an authentication protocol to allow access to a network, comprising:

a client electronic system (client) configured to perform a primary authentication protocol with a first network access point electronic system (first AP) in response to a first request to authenticate, wherein said client is configured to receive a key lease if said primary authentication protocol is successful, wherein said key lease includes context information, and wherein said client is configured to perform a secondary authentication protocol with a second network access point electronic system (second AP) using said key lease in response to a second request to authenticate.

48. An apparatus as recited in Claim 47 wherein if said secondary authentication is successful, said second AP uses said context information of said lease key to control access of said client to said network.

49. An apparatus as recited in Claim 47 wherein said context information includes information established in said primary authentication protocol.

50. An apparatus as recited in Claim 47 wherein said context information includes accounting information, session timeout information, and filtering information.

51. An apparatus as recited in Claim 47 wherein said key lease further includes a first identifier associated with said client, a first encryption key associated with said primary authentication protocol, a second encryption key for use in said secondary authentication protocol, a key lease period for indicating a length of time in which said key lease is valid, integrity function data for determining an unauthorized change to a first portion of said key lease, and a second identifier associated with a particular network access point electronic system group of a plurality of network access point electronic system groups.

52. An apparatus as recited in Claim 51 wherein said first portion includes said first identifier, said first encryption key, said second encryption key, said key lease period, and said context information.

53. An apparatus as recited in Claim 51 wherein a second portion of said key lease is encrypted using a third encryption key.

54. An apparatus as recited in Claim 53 wherein said second portion includes said first identifier, said first encryption key, said second encryption key, said key lease period, said context information, and said integrity function data.

55. An apparatus as recited in Claim 53 wherein said client is configured to transmit said first identifier and said key lease to said second AP, wherein said second

AP retrieves said third encryption key corresponding to said second identifier if said second AP is associated with said second identifier of said key lease, and wherein said second AP decrypts said second portion of said key lease using said retrieved third encryption key.

56. An apparatus as recited in Claim 55 wherein said second AP determines whether said first identifier transmitted by said client matches said first identifier decrypted from said key lease, determines whether said integrity function data decrypted from said key lease matches an integrity function performed on said first portion of said key lease, and determines whether said key lease period has not expired, and wherein if verification of said first identifier, said integrity function data, and said key lease period is successful, said second AP initiates said secondary authentication protocol with said client.

57. An apparatus as recited in Claim 47 wherein said secondary authentication protocol comprises a mutual challenge-response protocol based on symmetric encryption.

58. An apparatus as recited in Claim 47 wherein said secondary authentication protocol comprises a mutual challenge-response protocol based on a one-way hash function message authentication code (HMAC) implementation.

59. An apparatus as recited in Claim 47 wherein said secondary authentication protocol comprises a mutual challenge-response protocol based on a keyed message authentication code implementation.

60. An apparatus for performing an authentication protocol to allow access to a network, comprising:

a first network access point electronic system (first AP) configured to perform a primary authentication protocol with a client electronic system (client) in response to a first request to authenticate, wherein said first AP is configured to generate a key lease and transmit said key lease to said client if said primary authentication protocol is successful, wherein said key lease includes context information, and

a second network access point electronic system (second AP) configured to perform a secondary authentication protocol with said client using said key lease in response to a second request to authenticate.

61. An apparatus as recited in Claim 60 wherein if said secondary authentication is successful, said second AP uses said context information of said lease key to control access of said client to said network.

62. An apparatus as recited in Claim 60 wherein said context information includes information established in said primary authentication protocol.

63. An apparatus as recited in Claim 60 wherein said context information includes accounting information, session timeout information, and filtering information.

64. An apparatus as recited in Claim 60 wherein said key lease further includes a first identifier associated with said client, a first encryption key associated with said primary authentication protocol, a second encryption key for use in said secondary authentication protocol, a key lease period for indicating a length of time in which said key lease is valid, integrity function data for determining an unauthorized change to a first portion of said key lease, and a second identifier associated with a particular network access point electronic system group of a plurality of network access point electronic system groups.

65. An apparatus as recited in Claim 64 wherein said first portion includes said first identifier, said first encryption key, said second encryption key, said key lease period, and said context information.

66. An apparatus as recited in Claim 64 wherein a second portion of said key lease is encrypted using a third encryption key.

67. An apparatus as recited in Claim 66 wherein said second portion includes said first identifier, said first encryption key, said second encryption key, said key lease period, said context information, and said integrity function data.

68. An apparatus as recited in Claim 66 wherein said second AP is configured to receive said first identifier and said key lease from said client, wherein said second AP is configured to retrieve said third encryption key corresponding to said second identifier if said second AP is associated with said second identifier of said key lease, and wherein said second AP is configured to decrypt said second portion of said key lease using said retrieved third encryption key.

69. An apparatus as recited in Claim 68 wherein said second AP is configured to determine whether said first identifier transmitted by said client matches said first identifier decrypted from said key lease, to determine whether said integrity function data decrypted from said key lease matches an integrity function performed on said first portion of said key lease, and to determine whether said key lease period has not expired, and wherein if verification of said first identifier, said integrity function data, and said key lease period is successful, said second AP is configured to initiate said secondary authentication protocol with said client.

70. An apparatus as recited in Claim 60 wherein said secondary authentication protocol comprises a mutual challenge-response protocol based on symmetric encryption.

71. An apparatus as recited in Claim 60 wherein said secondary authentication protocol comprises a mutual challenge-response protocol based on a one-way hash function message authentication code (HMAC) implementation.

72. An apparatus as recited in Claim 60 wherein said secondary authentication protocol comprises a mutual challenge-response protocol based on a keyed message authentication code implementation.